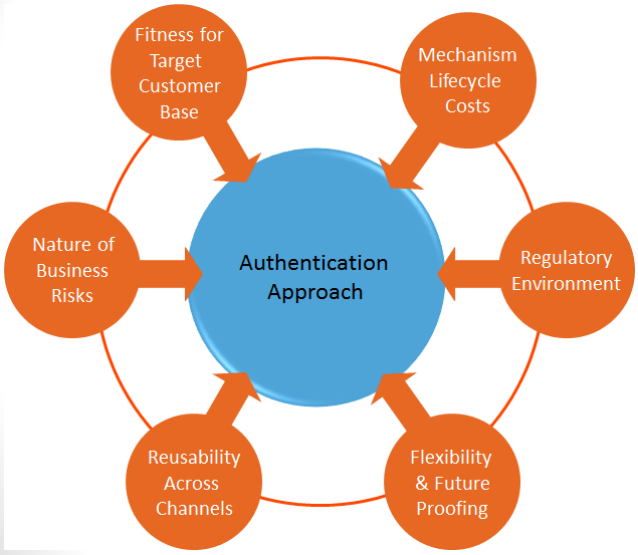
AUSCERT 2012 SECURITY ON THE MOVE

The imminent demise of specialised security tokens for user and transaction authentication

Ross Oakley, Salt Group

AusCERT 2012

Authentication mechanism selection



AusCERT 2012

Where it began

Thales Watchword II

One time password
AND
Signature Mode

…. specialised tokens were issued to a select few for securing high value transactions

- Threats were relatively unsophisticated and not systemic
- Total cost of tokens and issuance was not an issue
- Tokens were fit for purpose

When it began

In 1992 Internet banking did not exist !

AusCERT 2012

… and the world has changed

Business flexibility is more critical

- New transaction types and electronic delivery channels for all market segments
- Increased focus on self service for all market segments

Risk landscape is more hostile

- Explosion in Internet based transaction banking increases the target for attackers
- Attacks are diverse and prolific and increasingly sophisticated

Users are more demanding

- Usability is a key differentiator in e-service delivery

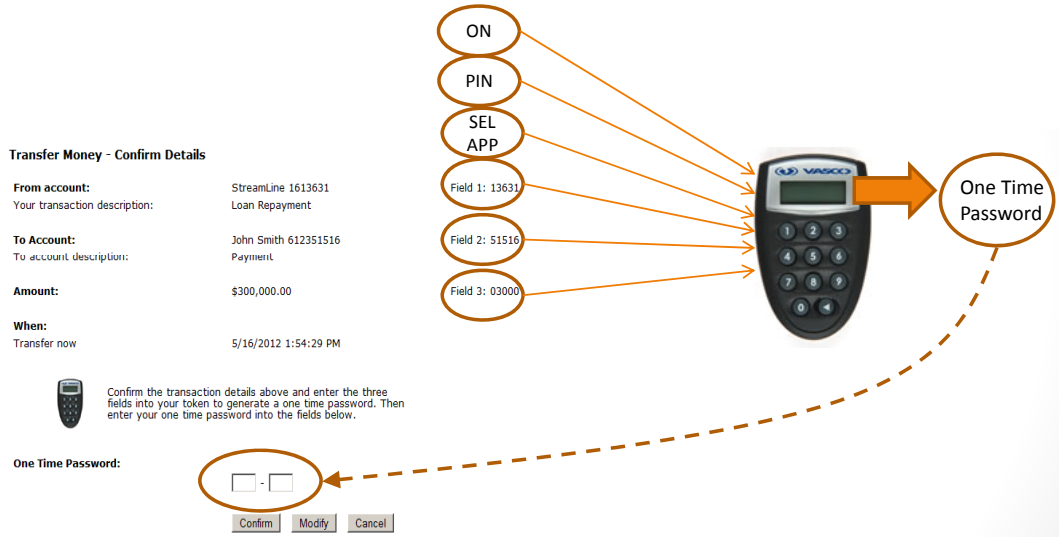
AusCERT 2012

… but the sad state is that many banks continue to deploy old world responses to modern threats to transaction security,

… it's the way it has always been done

AusCERT 2012

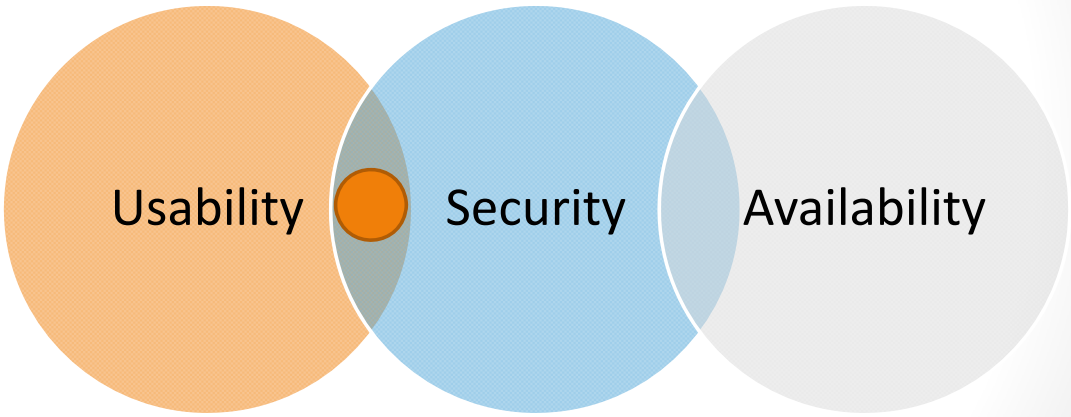
Specialised token usage



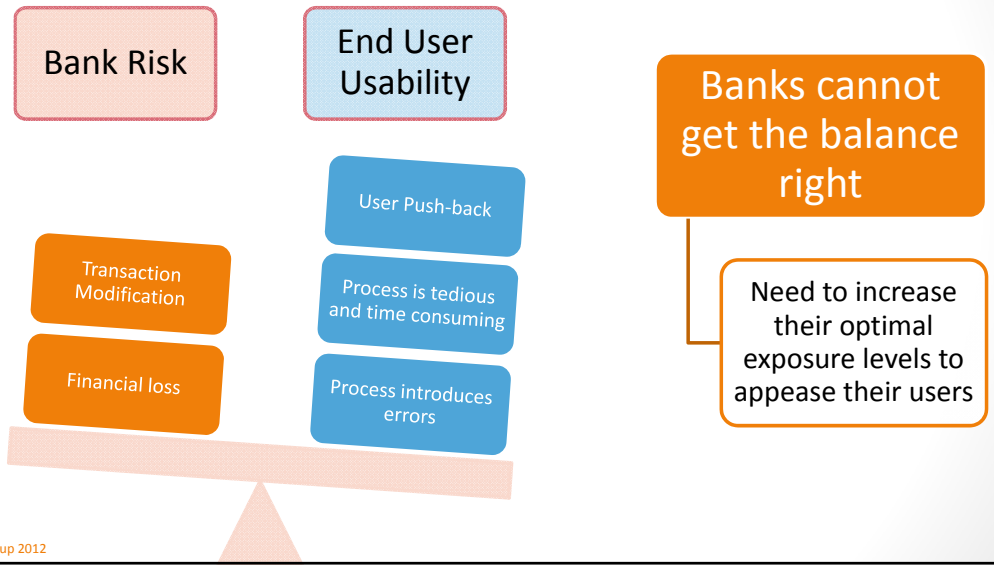
AusCERT 2012

... I expect that you can see some problems here

The pillars of online service delivery



… and the main trouble with specialised tokens is …



…. specialised tokens are a solution past

Bad user experience with input of around 24 characters required for typical payment	• User complaints affect authentication value threshold
Costly and cumbersome to deploy and manage	• Churn rate very high in retail environment • Significant lag time between registration and fulfillment
Token configuration is static	• Typically four "fields" (6-8 characters length) plus PIN • Inflexible for new transaction signature definition
Subject to malware social engineering attacks in the creation of the "field values" to be entered	• Tokens often require "real field" truncation to conveniently input into token (eg account number)
Token signature does not include transaction context	• Arguable value in dispute situation and may not include all critical transaction data due to truncation

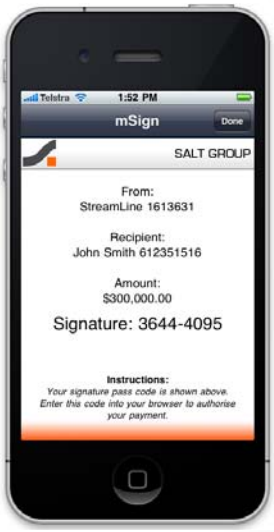
SALT mSign

mSign

An authentication model that addresses today's needs

High assurance transaction signing
- Brandable
- PIN Protected
- Any mobile device

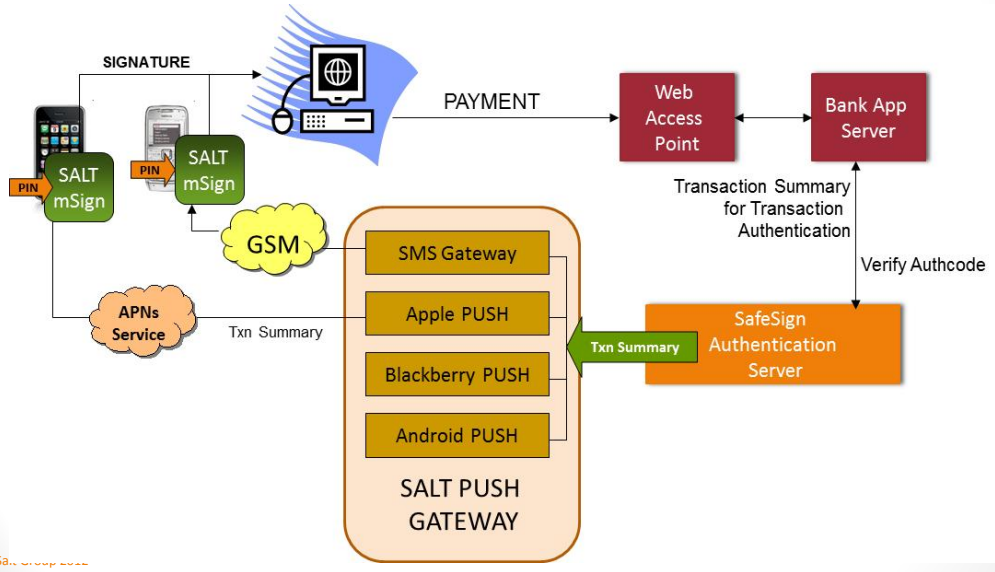
Supports "What you See is What you Sign" Workflow



AusCERT 2012

SALT mSign

SALT mSign for Transaction Signing - use case



AusCERT 2012

SALT mSign

mSign – addressing bank and user needs

No more annoying need for user entry of transaction data into a token

- Transaction summary sent to the handset over the air
- Intuitive user interface; the user "views" and "approves"
- Eliminates user keying errors
- Faster and less error prone than security token "signature" mode use

Free format "authentication data" frees up your security model

- Authentication fields / transaction summary determined by the host application; no set format
- Easy introduction of new transaction types – no impact on token
- Context is included in the signature for improved non repudiation
- Optional policy based inclusion of supplementary data input

AusCERT 2012

SALT mSign

Addressing Man in the Browser Attacks with Salt mSign Mobile Authentication

The Attack

- Man in the Browser attacks modify a user's transaction prior to submission to the bank, typically by changing the beneficiary account, at least.

Traditional Bank Responses

- SMS sent to the user for transaction validation.
- Specialised security tokens deployed to enable out of band transaction signature generation.

AusCERT 2012

The problems with SMS

- Mobile Number Porting
- Nobody reads the transaction summaries !!
  - Banks globally say that SMS delivered transaction summaries are not read properly.
    - Beneficiary account number changes by malware go undetected
    - Man in the Browser Malware developers know this and are not deterred from targeting banks that use SMS out of band transaction summary based authentication.

SALT mSign

mSign addresses both these threats

PUSH Message is not subject to mobile number porting

- PUSH is PKI scheme protected
- PUSH is to a device, not a mobile number

… critical authentication data is (optionally) confirmed by the user to avoid undetected malware attacks

Partial transaction summary displayed

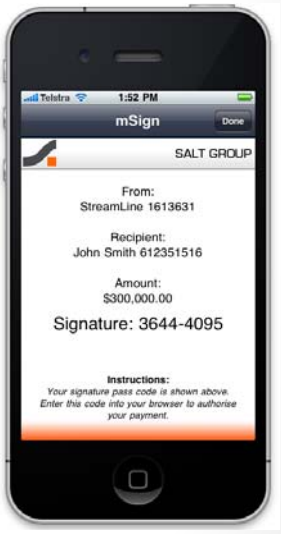
Supplementary information requested
- Determined by centralised policy based on risk
- User forced to refer to original documentation

AusCERT 2012

… the entire displayed transaction summary is protected by the Signature

Any input data inconsistency alerted to the bank
- Central response

What you see is what you have signed
- Includes context
- Incorporates user input data



AusCERT 2012

.... specialised tokens are a solution past

Bad user experience with input of around 24 characters required for typical payment	• User complaints affect authentication value threshold
Costly and cumbersome to deploy and manage	• Churn rate very high in retail environment • Significant lag time between registration and fulfillment
Token configuration is static	• Typically four "fields" (6-8 characters length) • Inflexible for new transaction signature definition
Subject to malware social engineering attacks in the creation of the "field values" to be entered	• Tokens often require "real field" truncation to conveniently input into token (eg account number)
Token signature does not include transaction context	• Arguable value in dispute situation and may not include all critical transaction data due to truncation

AusCERT 2012

SALT mSign fully addresses the weaknesses of specialised security tokens

Bad user experience with input of up to 20 characters required for typical payment	•Signature data is received over the air with mSign •Zero or limited supplementary info required to be input with mSign	SALT mSign
Costly and cumbersome to deploy and manage	•Over the air deployment and activation •Closed loop provisioning enables token usage within the same session	SALT mSign
Token configuration is static	•Signature data is unstructured with mSign •New transactions commissioning has no impact on mSign	SALT mSign
Subject to malware social engineering attacks in the creation of the field values to be entered	•Not applicable in mSign. Signature data is received from the bank via the independent PUSH channel	SALT mSign
Token signature does not include transaction context	•Full context is signed with mSign	SALT mSign

AusCERT 2012

The odd man out is ……..

Something to ponder on your journey home

Have a safe trip and thankyou for your attention

AusCERT 2012

www.saltgroup.com.au
roakley@saltgroup.com.au

Visit Salt Group with Thales eSecurity on Stand 66 to see mSign in action